

Index

Note to the reader: Throughout this index **boldfaced** page numbers indicate primary discussions of a topic. *Italicized* page numbers indicate illustrations.

Symbols & Numbers

! (exclamation point), in tool names, 144
 \$. file, 183
 %SystemRoot%\ntds directory, 77
 %SystemRoot% variable, 78
 >> (append operator), 145
 > (redirect operator), 145
 2703(f) orders, 10

A

access, vs. logon, 354
 access control list, 38
 access token, 57
 AccessData
 FTK imager, 261
 Registry Viewer, **207–211**, 208, 218
 for NTUSER.DAT file, 236
 account logon events
 bottom line, 493–494
 on non-domain controller, 383
 account management events, **399–409**
 logging, 331
 Account Operators group, 38
 accounts. *See* users and groups
 Active Directory, 25, 77, 362
 Active Directory Users and Computers
 Microsoft Management Console, 32, 32
 Administrators group, 38
 adding account to, 51–52
 Advanced Registry Trace (ART), 203
 Advanced Security Settings dialog box
 Auditing tab, 332
 Effective Permissions tab, 41, 41
 agency.jpg file, 462
 allocated cluster, 167
 alternate data streams, 186–187
 hiding data in, 189–190
 anchor points in reports, 456
 inserting in document, 458, 459
 antivirus software
 disabling, 224
 and malware tool, 277
 and testing platform, 274
 and tool analysis, 267
 append operator (>>), 145
 AppEvent.evt file
 database file structure, 433–437, 435
 properties, 436
 application layer firewall, log
 from, 11
 Application.evt log file, 327, 328–329
 examining events, **422–423**
 ARP cache-poisoning techniques, 102
 ASCII strings, from EnCase copy/
 unerase feature, 268

attacker

- changes in execution flow of process, 62
 - DLL injection, 62–66, 63, 65
 - hooking, 66–67
 - evidence from computer, 215
 - expertise level, 5, 270
 - exploiting, 265–266
 - former employee as, 298–299
 - and groups, 36
 - hiding evidence, 129
 - tools. *See* tools of attacker
 - use of inactive accounts, 14
 - use of nonstandard ports, 110
- \$AttrDef file, 183
- attribute byte, 173
- \$ATTRIBUTE_LIST MFT attribute, 180, 183
- attributes, 180–181
- audit policy change events, 416–417
- auditing, 32
 - bottom line, 423–424, 495–496
 - Windows settings for, 329–334
- authentication
 - vs. account logon, 361–364
 - centralization of logging, 383
 - mechanisms in Windows, 87–93
- authorized user, mass copy of files, and criminal activity suspicion, 379–380
- AutoComplete data, for Internet Explorer, 235
- AutoComplete Settings dialog (Internet Explorer), 235
- autorun.inf file, 463
- autoruns, to determine startups, 259–260, 260

B

- backdoor shell, in Hacker Defender, 73
- backup domain controller (BDC), 24
- Backup Operators group, 38, 403
- backups
 - of hive files, 206
 - of logs, 9
- \$BadClus file, 183
- batch file
 - for hidden data stream, 189–190
 - to run stored SQL queries, 321–323, 409
 - for stopped or started Security Center of Firewall query, 419
- BeatLM, 95
 - for cracking passwords, 100, 100–102
- Before The Installation of Hax Tools, 226
- bias, in incident reports, 8
- binary program, 56
- bit, 56
- \$Bitmap file, 180, 184
- bitmap file, for NTFS file system, 183
- \$BITMAP MFT attribute, 181
 - file creation and, 184
- bkhive, 104
- bkreg, 105
- blank password, hash for, 84
- bookmark output from EnCase
 - copying and tweaking, 430, 431
 - grouped by Created, 429
 - grouped by Event, 428, 428
- bookmarks in reports, 456
 - names for, 459

bookmarks, names for, 459
boot CDs, vs. live-analysis CDs, 131
\$Boot file, 183
boot process
 automatic startup from file outside
 Registry, 256–257
 Event ID for, 319
bots, 146
brute-force cracking, 102

C

cached logons, 248
Cain & Abel, 17, 102
 for decrypting Protected Storage
 System, 237
 and LSA secrets, 246, 247
Carvey, Harlan, 157
 Registry-parsing Perl scripts from,
 211
CaseMap, 463, 464
CaseSoft, 463
cd .. command, 173
change.log files, 228, 228
clear-text passwords, in swap file, 246
client, 22, 23
clipboard, copying log event to, 346, 374
cloning virtual machine, 280–281
clusters
 in FAT12 system, 164
 in FAT32 system, 165
 in NTFS partition, 183
 unallocated or allocated, 167
 wasted space in, 166
code, 56
 monitoring from attacker, 273–282
command prompt
 for Log Parser, 317
 Open Command Window Here tool
 for, 268, 313–314, 314
 for starting new process, 64
command shell, on CD, 135
communication between computers
 monitoring, 146–148, 147
 numbers used to identify, 108
compiler, 56
compiling, 56
compromised files, determining
 accounts with permissions to access, 41
compromised host, for intruder
 toolbox, 264
computer
 as criminal tool, v
 not in domain, user accounts for, 33
 pulling the plug, 132
computer accounts, 400
Computer field, in event logs, 338, 349
Computer Management console, local, 33
connecting computers, 21–23
connection, current state of, 113–114
corrupted event log database
 if open and not synchronized, 440
 repairing, 444–446
court testimony
 about technical matters, 466–467
 credibility with jury, 45
 minimizing complexity for, 341
cracking passwords
 offline, 102–103
 on running systems, 79–82, 80
 with ScoopLM and BeatLM, 96–102

credibility with jury, 45
criminal activity
 by former employees, 298–299
 mass copy of files by employee,
 379–380
 recreating, 416
cross-platform file system, 163
cross-platform forensic artifacts, 164
.csv files
 importing to CaseMap, 464
 for saving event log, 340
CurrentControlSet key, 204
custom text style, for MFT records in
 EnCase, 179, 179

D

daemons, 109–110
damage by intrusion, mitigating, 266
Data Encryption Standard (DES), 81
data exchange, in trust relationship, 27
\$DATA MFT attribute, 181, 182
 file creation and, 184
 multiple, 186–188
data stream, syntax for addressing, 187
database
 evaluating attacker impact on,
 414–415
 repairing corrupted event log,
 444–446
database slack, 433, 434
date and time information. *See* time
 stamps
Date field, in event logs, 335–336
decode.exe, 249

default administrator local user
 account, 35
Default FTP site properties dialog, 302
 Extended Properties tab, 303
 General Properties tab, 303
default groups, 36, 37
default settings, for security event
 auditing, 334, 354
default user accounts, 33
Default Web Site option, for IIS, 290
Default Web Site Properties dialog box,
 290, 290–291
defense attorneys, 45
deleting
 alternate data streams, 188
 files
 auditing attempts, 333, 333
 from FAT file system, 170
 in NTFS, 185
 Windows accounts, vs. disabling,
 359
denial of service attack, 46
Dependency Walker, 271, 271–272, 279
depends.exe, 271
DES (Data Encryption Standard), 81
Description field, in event logs,
 344–345
destination Internet Protocol (IP)
 address, 108
destination port, 108
device drivers, 71
 Event IDs 7036 and 7036 for, 420, 421
DHCP (Dynamic Host Configuration
 Protocol), 264
 port, 116

- server logs, **306–310**
 - event ID codes, 308
 - fields in record, 308
 - log format, 307
- dictionary-based attacks, 79
- digital evidence
 - destruction, 13
 - search warrant for, 15, 16
- directories
 - default, for IIS logs, 291
 - “dot double dot” structure, 173, 173
 - structure in Windows, 162
- directory entry
 - in FAT, 172, 172–173
 - in FAT file, 168, 169
- directory services, logging events, 331
- disabled user accounts, 33
 - vs. deleting, 359
- disconnecting, to end Remote Desktop, 389
- discovery of attack, information on, 4
- distribution groups, for domain controllers, 406
- DLL injection, **62–66**, 63, 65
 - real world scenario, **68–69**
- DLLs. *See* dynamic-link libraries (DLLs)
- \Documents and Settings
 - \All Users\Start Menu,
 - \Programs\Startup, 256
 - \%UserName%\Start Menu,
 - \Programs\Startup, 256
- domain accounts, 33–34, 362
 - attacker information on, 381
- domain administrator account, 34
- Domain Admins group, 38
- domain controllers (DCs), 23–24, 25, 383
 - account information stored by, 33
 - account logon event generation on, 370
 - attacker interest in, 381
 - as authenticating computer, 362
 - authentication for logon, 369
 - change to Group Policy on, 417
 - compromise to, 87
- domain logon, 95
- domain tree, 26, 26
- domains in Windows, **23–29**
 - determining type, 24
 - interconnecting domains, **25–27**
 - local accounts in, 35
 - state of, 378
- Dorian Software, 422
- “dot double dot” directory structure, 173, 173
- .DS_Store file, 164
- Dynamic Host Configuration Protocol (DHCP)
 - port, 116
 - server logs, **306–310**
 - event ID codes, 308
 - fields in record, 308
 - log format, 307
- dynamic IP address, interface for configuring, 249, 249
- dynamic-link libraries (DLLs), 56–57, 60, 61
 - on live analysis CD, 133
 - preparing DLLs, 134–135

E

e-mail

- to cause authentication attempt, 97
- Hypertext Markup Language (HTML) in, 94–95
- \$EA MFT attribute, 181
- \$EA_INFORMATION MFT attribute, 181
- EAPOL (Extensible Authentication Protocol Over LANS), 250
- Edit mode, for EnCase Notes
 - bookmark, 429, 429
- Edit Term dialog, 431
- EFSDump, 105
- Elcomsoft, Advanced Registry Trace (ART), 203
- Election Communications Privacy Act, 10
- electric power, pulling the plug, 132
- electronic format for reports, 455–456
- embedding, 46
- employees, former, criminal activity by, 298–299
- EnCase, 103, 150
 - 32-byte directory entries decoded by, 168
 - associating security ID with volume in, 233
 - bookmark output when grouped by Created, 429
 - bookmark output when grouped by Event, 428, 428
 - conditions, 189
 - display of data decrypted from Protected Storage Area, 211

- to display open ports, 155, 156
- to examine Windows event logs, 425–433, 426
- hidden data streams in, 189, 189
- MFT record numbers in, 179, 179
- for parsing event log fragments, 452, 452
- for recovery of event log, 449, 450, 451
 - starting in Console Mode, 152
- EnCase Computer Forensics: The Official EnCE: Encase Certified Examiner Study Guide*, 241
- EnCase Enterprise, Mobile Enterprise Edition, 150
- EnCase FIM (Field Intelligence Model), 140, 150–157
 - to view snapshot data, 154–155, 155
- Encrypting File System (EFS), 102–103
- encryption, 140
- EnScripts
 - for bookmarked report of startup locations, 258, 258
 - for examining event logs, 425
 - for extracting time zone offsets, 253
 - for Registry, 206
 - Scan Registry, 207, 207
 - Sweep Enterprise, 153, 153
 - Windows Initialize Case, 206, 218
- Enterprise Admins group, 38
- Event Analyst Service, 247, 422
- Event field, in event logs, 337
- Event ID number
 - 1, custom messages sent to, 422
 - 528 for logon event, 354, 355, 364, 365, 386

- 528 for logon event using RDP, 388–389
 - 529 for mistyped password or username, 358, 358, 365
 - 535 for expired password, 360
 - 538 for successful logoff, 356, 365, 370, 379, 390
 - 539 for locked account logon attempt, 360
 - 540 for network logons, 364, 364, 365, 380–381, 386
 - 560 for remote file access, 412, 414
 - 560 for request to open file handle, 410, 410–413, 411
 - 562 for closed handle, 413, 413
 - 567 for WriteData access method per file handle, 415
 - 612 for audit policy change, 417
 - 612 for current audit policy, 416
 - 624 for account creation, 400
 - 626 for account enabled, 402, 408
 - 630 for account deletion, 408
 - 636 for enabled group member addition, 403, 406
 - 637 for group membership changes, 406
 - 642 for account changes, 400, 401, 405
 - 644 for recording account lockouts, 406–407, 407
 - 671 for manually unlocking account, 407
 - 672 for TGT, 372, 372, 375, 376
 - 673 for issuance of service ticket, 374–375, 375, 376, 376, 380, 381, 395
 - 675 for failed Kerberos authentication, 376, 385–386, 395
 - 676 for failed Kerberos authentication, 385–386, 395
 - 680 for authentication of domain account, 370, 373, 376, 384
 - 681 for failed authentication, 368, 370, 376, 384, 392
 - 682 for user reconnection, 391
 - 683 for user disconnect, 391
 - 6005 for boot, 319
 - 6005 for event log service start, 421
 - 6006 for event log service stop, 421
 - 7035
 - for service start signal, 418
 - for service stop signal, 417
 - 7036
 - for started service, 418
 - for stopped service, 417
 - and event log Description field contents, 345
 - for failed attempts to logon, 358, 365
 - for group membership, 404
 - for logons, 354
 - reference site, 409
 - for shut down, 319
 - in Windows event log, 336, 341
- event logs. *See* Windows event logs
- Event Properties dialog, 344
- for account being enabled, 402
 - for account creation, 400, 400
 - copying contents to clipboard, 374
 - with Description field, 344, 355
 - for Remote Desktop Protocol connection, 386

- Event Rover, 422
 - report, 423
 - Event Viewer, 328, 328
 - Action menu, 339
 - Clear All Events option, 447, 448
 - context sensitivity of menu options, 338, 339
 - copy button in Event Properties window, 346
 - file name display in, 343, 343–344, 344
 - Find feature, 350, 350
 - launching, 328
 - saving and opening log files, 339–340
 - searching with, 347–351
 - Security.evt log file in, 336, 337
 - for System event log contents, 335, 335
 - using, 324–347
 - View menu, 347
 - Event Viewer User field, 444
 - eventlog service
 - Properties dialog, 433
 - stopping, 434
 - Everyone group
 - auditing, 333
 - Full Control vs. Read permission, 42
 - evidence. *See also* Registry evidence analysis, 13–15
 - collection, 11–13
 - digital sources, 11
 - of employee copying files, 414
 - finding in memory, 129–131
 - identification and preservation, 8–9
 - locating all, 394–395
 - location for, 16
 - ports as, 111–117
 - requirement to preserve, 10
 - suggestions for preserving, 5
 - .evt file extension, 327
 - for saving event log, 340
 - examiner.htm file, 462
 - Excel spreadsheet
 - for analyzing EnCase results, 432–433
 - from EnCase Windows Event Log Parser, 427
 - exclamation point (!), in tool names, 144
 - executables, 56–57
 - execution flow, 59, 60
 - expired password, 360
 - Exploit, 17
 - exploit command (Metasploit), 49, 50
 - exporting event logs with EnCase, 427
 - \$Extend file, 183
 - Extended Logging Properties dialog box, 291
 - Extended Properties tab, 292
- F**
- failed account logon, 358, 358
 - Event Properties dialog for, 344, 345
 - failed attempts, logging, 331
 - FAT (File Allocation Table), 162, 164–177
 - deleting file from, 170
 - locating directory entry fragments, 176–177
 - MAC times for, 173–174

- FAT1 table, 166
- FAT2 table, 166
- FAT32 filesystem, 39, 165
- Federal Rules of Evidence, exception
 - for hearsay rule for log evidence, 9
- file fragmentation, preventing, 433
- file permissions, 38, **39–41**
 - reconciling with share permissions, **39–41**
- file Properties dialog box
 - for attributes, 175
 - permissions set in, 38
- file record, 178
- file slack, 166
- file status byte, repairing, 445
- file systems
 - bottom line, 190–191, 478–480
 - vs. operating systems, **161–164**
 - performance requirements, 163
 - for Windows, 162
- File Transfer Protocol (FTP)
 - and ADS loss, 187
 - parsing logs, **300–306**
 - field data, 304–305
 - number inside brackets, 306
 - sc-status field, 301–302
- Filemon tool, 133, 139, 141, 274
- \$FILE_NAME MFT attribute, 180, 181
 - file creation and, 184
- %filename% variable, for batch file, 321
- files
 - access events, **409–415**
 - auditing access to, 334
 - deleting
 - from FAT file system, 170
 - in NTFS, 184
 - files currently opened for use by remote users, 137
 - logical vs. physical size, 166
 - permissions to access, 71
 - recovering
 - after deleting, 171–172
 - encrypted with EFS, 102–103
 - in NTFS, 185–186
 - requesting from computer forensics examiner, 259
- filtering
 - in EnCase, 426
 - event logs, 347–349
 - remembering to remove, 349
 - Log Parser query, 317–318
 - in regmon.exe, 201, 201
- Find feature, in Event Viewer, 350, 350
- finding event logs from free space, **446–451**, 450
- firewalls, 11, 150. *See also* Windows Firewall
- floating footer in event log file database, 436, 438
 - comparing to header, 438–439, 439
 - locating, 438
- floppy disks
 - redirecting output to, 144–145
 - Windows NT Rescue, 77
- Folder Options dialog box, 176, 176
 - View tab, 40, 40
- folder properties
 - permissions set in, 38
 - Sharing tab, 42, 43

folders and files. *See also* directories;
files
 requesting from computer forensics
 examiner, 259
Forensic Server Project, 157–158
Forensic Toolkit (FTK), 207
forest, 26, 27
formatting partitions, 165
former employees, criminal activity by,
 298–299
Foundstone, SuperScan, 149, 284, 285
FPort utility, 69, 138, 139
fragmented files, 172
free speech, 51
FrontPage (Microsoft), 457, 457
 highlight tool, 459
FTK imager, 261, 446
FTP logs, parsing, **300–306**
 field data, 304–305
 number inside brackets, 306
 sc-status field, 301–302
Full Control, for Everyone group, 42
functions, 59

G

getmac.exe command, 251
ghost image, 273
gif format, 462
Giuseppini, Gabriele, 313
global groups, for domain controllers,
 406
glossary.htm file, 462
Google, for string in hacker's tool, 270
Google toolbar, searches stored in
 Registry for, 240, 240

graphical user interface (GUI), for
 Windows, 55
Greenwich Mean Time (GMT), 206, 251
 for IIS log time stamps, 291
GREP search, for FAT entry fragments,
 176–177
Group Policy, 25
 for enabling auditing, 329
 forcing use of only signed device
 drivers, 71
groups
 Event IDs for, 402–403
 Event IDs for membership, 404
 limited to domain controllers, 406
 membership changes, 406–407
GUID-named interface, information
 from, 250
Guidance Software. *See* Encase

H

hack example, **45–53**
hacked system, information from
 monitoring, 146–147
Hacker Defender, 73–74
hacker tools, as evidence, 17
hackers. *See* attacker
handles to objects, 410
hardening the system, 112
hash analysis, 74
 techniques, 17
hash functions, 78
hash value of password, 78
header in event log files, 434, 435, 436
 comparing to footer, 438–439, 439

- Helix, 157
- hiberfil.sys file, 246
- Hidden attribute, 175
- hidden files, displaying, 176
- hidden metadata files, from operating system, 164
- hiding data, 186–187
- high-level programming languages, 56
- history files, on suspect computer, 18
- hive files
 - backups of, 206
 - mapping names to restore point filenames, 229
 - path of, 205
 - visibility of, 204
- hives, 195, 197
- HKEY_CLASSES_ROOT, 196
- HKEY_CURRENT_CONFIG, 196
- HKEY_CURRENT_USER, 196
 - \Software, 216
 - \Google\NavClient\1.1\History, 240
 - \Microsoft\Windows\CurrentVersion\Explorer\RecentDocs, 239
 - \Microsoft\Windows\CurrentVersion\Explorer\RunMRU, 238
 - \Microsoft\Windows\CurrentVersion\Explorer\UserAssist, 241
 - \Microsoft\Windows NT\CurrentVersion\Winlogon, 256
 - \Yahoo\Companion\SearchHistory, 241
 - common startup locations in, 255
- HKEY_LOCAL_MACHINE, 197
- HKEY_LOCAL_MACHINE
 - \Hardware, 197, 198, 203
 - HKEY_LOCAL_MACHINE
 - \SOFTWARE, 216–220
 - \Microsoft\EAPOL, \Parameters\Interfaces, 250
 - \Microsoft\Security Center, 222
 - \Microsoft\Windows
 - \CurrentVersion\App Paths, 217
 - \CurrentVersion\Policies\System, 220
 - \CurrentVersion\Uninstall, 217
 - \Microsoft\Windows NT
 - \CurrentVersion, 162
 - \CurrentVersion\ProfileList, 234, 234
 - \CurrentVersion\SystemRestore, 225
 - \CurrentVersion\Windows, 257
 - \CurrentVersion\Winlogon, 218, 219–220, 248
 - \Microsoft\WZCSVC, \Parameters\Interfaces, 250
 - common startup locations in, 253–254
 - HKEY_LOCAL_MACHINE\SYSTEM
 - \ControlSet001\Control
 - \ComputerName\ComputerName, 249
 - \Network, 250

- \CurrentControlSet\Control
 - \hivelist, 199
 - \Terminal Server, 212
 - \TimeZone Information, 252, 252
- \CurrentControlSet\Services, 122, 122–123, 224
 - \SharedAccess\Parameters\FirewallPolicy, 223
 - \Tcpip\Parameters\Interfaces, 246–247
- common startup locations in, 254–255
- HKEY_USERS, 197
 - hive keys and corresponding files, 198
- honeypots, 12, 146–147
- hooking, 66–67
- hostname of web server, 290
- HTML (Hypertext Markup Language)
 - code for hyperlink, 458
 - in e-mail, 94–95
 - for narrative report, 456–457
- HTTP (Hypertext Transfer Protocol), 94
 - port for, 108
- hubs, 148
- hybrid rootkits, 73
- hyperlinks
 - basics, 456
 - code for hyperlink, 458
 - creating, 457, 460, 460, 461
 - creating narrative report with, 455–460

I

- IACIS (International Association of Computer Investigation Specialists), 157
- IANA (Internet Assigned Numbers Authority), 296
- IAT (Import Address Table), 60
- IIS Management Console, 289, 290
 - Implementing CIFS: The Common Internet File System* (Hertel), 87
- Import Address Table (IAT), 60
- IN operator, in Log Parser query, 318
- in-use bit flag, 186
- incident information, 7–8
 - Incident Response and Computer Forensics* (Prorise, Mandia and Pepe), 6
- InCtrl5, 274, 275
 - report, 279–280
- \$INDEX_ALLOCATION MFT
 - attribute, 181, 182, 185
- index.htm file, 462, 463
- \$INDEX_ROOT MFT attribute, 181, 185
- .ini file, for Hacker Defender, 74
- initial vetting, 3–5
- initiation of case by phone, 4
- Insert Hyperlink dialog, 458
- inside users, attacks by, 4
- installing IIS, on Windows XP Professional, 290
- interactive logon, 95, 355
- Internet Assigned Numbers Authority (IANA), 296

Internet Explorer

- AutoComplete data for, 235
- URL entry in Address field, 241

Internet Information Services (IIS)

- installing on Windows XP
 - Professional, 290
- logs, **289–299**
 - record details, 297–298
 - W3C Extended Log File Format, 291–298

Internet Protocol (TCP/IP) Properties dialog, 202

Internet Security Association and Key Management Protocol, port, 116

Intranet web servers, security for, 299

intruder. *See* attacker

intrusion detection systems (IDSs), 11

intrusion response, 6

investigations, tools, vii

investigative challenges, **18–19**

investigator, need to explain technique reasons, vi

IP addresses

- 0.0.0.0, 115
- 127.0.0.1, 115
- private space, 296
- recording in log, 395
- in Registry, **246–249**
- source and destination, 108
- for workstation, 414

ipconfig/all command, 250–251

IRC chat room, 18

J

John the Ripper, 85, 85–87

journaling file system, NTFS as, 177

jump-through machine, 146

jurisdiction, 4

jury, credibility with, 45

K

Keberos Ticket Granting Ticket service, 372

Kerberos, 87, 92–93, 371, 371–372, 373

audit events from failure, 385–386

clock skew, 377

Microsoft implementation, 93

port, 117

Kernel mode, 70

key pane, in Registry editor, 196

keymaster, for EnCase FIM, 153

keys in Registry, 195

killer.bat file, 420

Knoppix project, 157

known plain-text attack, vulnerability to, 89, 89

L

LanMan authentication, 87, 88, **88–91**, 89

LanMan (LM) hash, 78, 80–81

disabling, 82

vs. LanMan authentication, 88

last accessed times, for FAT files, 174, 174–175

“last known good configuration,” for Registry, 193

last logon, Registry evidence on, **218**, 219

layer-2 switches, 148

lease in DHCP, 306

- least privilege, 30
- legitimacy of incident report, 3
- libpcap.dll, 268
- Lightweight Directory Access Protocol, port, 117
- Linksys wireless router, accessing
 - DHCP logs on, 309
- listening port, process identifier (PID)
 - of process bound to, 115
- listening processes, 109
- live analysis
 - bottom line, 158–159, 477–478
 - collecting output from, **142–145**
 - with commercial products, **150**
 - documentation, 131
 - finding evidence in memory, **129–131**
 - with free products, **157–158**
 - key components, 130
 - tools, 276
 - care in selecting, 141
 - FPort utility, 138, 139
 - PsTools suite, 137–138
 - Whoami tool, 136, 136
- USB drives for, 143
- Windows CDs, **131–145**
 - burning, 136
 - creating for Windows XP, **134–136**
 - dynamic-link libraries (DLLs), 133
 - selecting tools for, **133–138**
 - steps for creating, 132–133
 - using, **142–145**
 - verifying, **139–140**
- Live View, 103
- LiveWire Investigator, 150
- LM (LanMan) authentication, 87, 88, **88–91**, 89
- local accounts, 33
 - authentication to, 367
- local Administrators group, account added to, 406
- local computer account
 - attacker targeting of, 384
 - reasons to use, 383–384
- Local Computer Policy, for security event auditing, 329, 330
- local logon, 95
- Local Security Authority (LSA), 245
- Local Security Authority System Service (LSASS), 248
- Local Security Settings MMC, 330
- location, of attackers, 14
- locked accounts, from incorrect password attempts, 406
- logevent.exe, 422
- \$LogFile file, 183, 185
- logged-on user, reports on current, 136
- \$LOGGED_UTILTY_STREAM MFT attribute, 181
- logging, 177
- logical size of file, 166
- logon banners, **219–220**
- logon events, **353–361**
 - vs. authentication, **361–364**
 - bottom line, 397, 493–494
 - logging, 331
- logon GUID, 356, 386, 387

Logon ID field, to correlate logoff event
with logon, 357, 357

Logon Type, in Event Properties
description, 355, 356

logon, vs. access, 354

logons
cached, 248
Microsoft terminology, 95

logs. *See also* Microsoft Log Parser;
Windows event logs
of account access, origins, 353
Application.evt log file, 327,
328–329
examining events, 422–423
backups of, 9
bottom line, 324–325, 488–492
DHCP Server, 306–310
event ID codes, 308
fields in record, 308
log format, 307
distributed nature, as
security, 381
evidence in, 11
from FTP, 300–306
field data, 304–305
number inside brackets, 306
sc-status field, 301–302
gaps in, 14
from network, 9
parsing from IIS, 289–299
priority of, 9
System.evt log file, 327, 329
in Event Viewer, 335, 335
examining events, 417–422

Windows event logs
EnCase to examine, 425–433
finding and recovering from free
space, 446–451, 450
internals, 433–444
repairing corrupted databases,
444–446
from Windows Firewall, 223,
310–312
loopback address, 115
LSA (Local Security Authority), 245
lsadump2 tool
and LSA secrets, 246
for password dumping, 247

M

MAC (Media Access Control) address
for network interface card, 309
resolving, 250

Mac OS X
file system support, 163
metadata files from, 164

MAC times, for FAT, 173–174

machine language, 56

Macs, RDP client for, 388

“magic number,” 441

malware (malicious software),
14–15, 102
modifying firewall to allow,
223–224
in Registry Viewer, 245
spoofed emails with, 58

Mandia, Kevin, 157

Mandiant, 157

- manufacturers, resolving MAC addresses to, 309
- Map Network Drive MRU key, 238
- mass rooter, 17
- Master Boot Record, 165
- Master File Table (MFT) system, 178–179
 - file record, 180
- Mastering Windows Server 2003* (Minasi), 333, 402, 409
- MD4 hash algorithm, 91
- meeting with victim organization, 5–10
 - evidence identification and preservation, 8–9
 - incident information, 7–8
 - meetings about, 5
 - victim network information, 6–7
- member servers, 23
- memory
 - data stored in, 12
 - division, 70
 - finding evidence in, 129–131
 - initializing, 57
 - management within Kernel mode, 70
 - space for processes, 57
- memory-only rootkit, 73
- “message separator,” 441
- Metasploit Console, 47, 47
- Metasploit Framework, 46–47
 - DLL injection attack with, 68
 - exploit phase of attack, 64
 - payload, 64
- methods, 59
- \$MFT file, 178, 183
- \$MFTMirr file, 183
- Microsoft
 - digital signature for device drivers, 71
 - libraries of code, 56
 - logon terminology, 95
- Microsoft Certified Systems Engineers, 21
- Microsoft FrontPage, 457, 457
 - highlight tool, 459
- Microsoft Global Catalog, port, 117
- Microsoft Help and Support, for codes in Event Properties description, 356
- Microsoft IIS Log File Format, 300
- Microsoft Log Parser, 289, 313–320
 - advanced techniques and queries, 321–323
 - DATAGRID output, 315
 - filter for query, 317–318
 - help function, 316, 316
 - opening command prompt for, 314, 315
 - queries
 - for account management events, 408–409
 - broad, 396
 - for device drivers Event IDs, 420–421, 421
 - for Event ID 673 entries, 382
 - for Event ID 680 and 681 entries, 384
 - IN operator, 318
 - ORDER BY clause, 318
 - parts, 316

- for stopped or started Security Center of Firewall, 419, 419
- WHERE clauses, 318
- in Sweep Case Options dialog, 427
- Microsoft Log Parser Toolkit* (Giuseppini and Burnett), 313, 323
- Microsoft Network Monitor format, 323
- Microsoft networks
 - bottom line, 52–53, 471–472
 - connecting computers, 21–23
 - hack example, 45–53
 - investigative challenges of, 18–19
 - organizational units, 29–31, 30
 - permissions, 37–45
 - file permissions, 39–41
 - reconciling share and file permissions, 43–44
 - share permissions, 42
 - users and groups
 - groups, 34–37
 - types of accounts, 31–34
 - Windows domains, 23–29
 - interconnecting domains, 25–27
- Microsoft Portable Executable File format (PE format), 56–57, 60
- Microsoft Security Bulletin 03-026, 49
- Microsoft Windows Internals* (Rusinovich and Solomon), 55, 118
- Microsoft Word, 457
- monitoring, for future illegal activity, 12
- MRU (most recently used) key, 236, 238–239
- My Computer, Properties, System Restore tab, 194

N

- names
 - for bookmarks, 459, 459
 - changing for tools, 135
 - of computer, from Registry, 249
 - of restore points, 226–227
- namespace, for domain parent-child relationship, 26
- narrative report with hyperlinks, creating, 455–460
- NAT Traversal protocol, port, 117
- NBT Session Service, port, 117
- nested groups, 38
- net localgroup command, 52
- net stop command, 224, 418
- net users command, 51
- NetBIOS over TCP (NBT) Name Service, port, 116
- netcat command, 283
- netstat command, 112–114, 113, 284, 285
 - for live analysis, 132
 - name resolution by, 113, 114
 - output from, 113, 114
 - for port information, 114–115
 - results in numeric format, 114
- Network Information Service master server, 24
- network interface card (NIC), MAC address for, 309
- network investigation
 - analyzing suspect's computers, 15–18
 - bottom line, 19–20, 469–471
 - evidence analysis, 13–15

- evidence collection, **11–13**
 - initial vetting, **3–5**
 - meeting with victim organization, **5–10**
 - evidence identification and preservation, **8–9**
 - expectations and responsibilities, **10**
 - incident information, **7–8**
 - victim network information, **6–7**
 - network logon, **95, 355**
 - caution for, **358**
 - network monitor, **147**
 - Network Neighborhood, **42**
 - network resources, permissions for, **38**
 - Network Time Protocol, port, **116**
 - network traffic monitoring, **146–148**
 - from attacker tools, **282–283, 283**
 - networks. *See also* Microsoft networks
 - topology of, **6**
 - New Technology LanMan (NTLM)
 - authentication, **87, 91–92, 367**
 - failed, on Windows 2000 system, **369**
 - LM authentication inclusion with, **92**
 - Nmap, **17**
 - non-domain controller, account logon events on, **383**
 - Notepad
 - for creating batch file, **189–190**
 - to display data hidden in ADS, **188**
 - NT LanMan (NTLM) hash, **78, 80**
 - ntds.dit file, **25, 77, 78**
 - NTFS (New Technology Filesystem), **162, 177–186**
 - creating, deleting and recovering data in, **184–186**
 - data structures, **178–183**
 - and permissions, **39**
 - system files, **183**
 - NTFS5, for Windows 2000/XP, **177**
 - NTUSER.DAT file, **232, 234**
 - viewing in EnCase, **204**
- O**
- \$OBJECT_ID MFT attribute, **180**
 - objects
 - access events, **409–415**
 - logging access to, **332**
 - one-way functions, **78**
 - Open Command Window Here tool, **268, 313–314, 314**
 - open port
 - scanning for, **149**
 - vulnerability from, **111**
 - open-source intelligence gathering, **16**
 - operating systems, vs. file systems, **161–164**
 - ORDER BY clause, in Log Parser query, **318**
 - organizational units, **29–31, 30**
 - Organizationally Unique Identifier (OUI), **309**
 - organized crime, v
 - oxid.it, **102**
- P**
- packet32.dll, **268**
 - paper reports, **455**
 - parent-child relationship, for domains, **26**

- parent directory, changing to, 173
- partitions, 162
 - formatting, 165
- passdump.exe, 247
- Password Recovery Toolkit (PRTK), 207
- password-sniffing attacks, 95
- passwords
 - adding “salt” to, 81–82
 - bottom line, 106, 474–475
 - clear-text, in swap file, 246
 - for computer accounts, 32
 - cracking
 - offline, **102–103**
 - on running systems, **79–82, 80**
 - with ScoopLM and BeatLM, 96–102
 - on Windows Server 2003 domain controller, 83–87
 - harvesting, 46
 - hash for blank, 84
 - lifetime limits, 82, 360
 - for local administrator, 35
 - locked accounts from incorrect attempts, 406
 - log file and, 359
 - from Registry Viewer, 210, 210
 - storage in Windows, **77–78**
 - tools for dumping, 247
- patches
 - and ports, 112
 - from vendors, 45
- path, of Registry hive files, 205
- payload, 47
- peer-to-peer network, 23
- permissions, **37–45**
 - for \System Volume Information folder, 226
 - file permissions, **39–41**
 - for files, 411
 - reconciling share and file permissions, **43–44**
 - vs. rights or policies, 38
 - share permissions, **42**
- persistent rootkit, 73
- Pest Patrol, **265–266**
- phishing scheme, 111
- Physical Disk Emulator module, 103
- physical size of file, 166
- plain-text attack, known, vulnerability to, 89, 89
- policies
 - for domain, 23
 - centralized control, 25
 - vs. rights or permissions, 38
 - logging changes to, 331
- port scanner, 17
- portability of domain account, 33
- Portable Executable File format (PE format), 56–57, 60
- ports, **107–111**
 - 443 for secure web traffic, 320
 - 4444, opening listener on, 49
 - 4445 for EnCase, 152
 - 31337, hacker interest in, 118–119, 121
 - bottom line, 124–125, 475–477
 - EnCase to display open, 155, 156
 - as evidence, **111–117**
 - external scans, **284–285**

- opening, 115
- and patches, 112
- scanning for open, 149
- Transmission Control Protocol (TCP), 117
- User Datagram Protocol (UDP), 116–117
- vulnerability from open, 111
- well-known, 108, 109, 110, 116
- power, turning off, and lost evidence, 130
- PowerPoint, timeline sent to, 465, 465, 466
- PowerToys for XP, 268
- preservation request, 10
- primary domain controller (PDC), 24
- privilege, groups to increase, 38
- privilege modes, 70–72
- procedures.htm file, 462
- process identifier (PID), of process
 - bound to listening port, 115
- processes, 57
 - command prompt for starting new, 64
 - displaying currently running, 118, 118
 - log for troubleshooting, 332
 - port associated with, 109
 - redirecting flow, 59–67
 - request for multiple handles, 412
 - security context for, 94
 - vs. services, 110
- processor, 56
 - privilege modes, 70
- ProDiscover, 150
- program, 56

- Properties dialog of files and folders,
 - Security tab, 39, 39, 40
- Protected Storage Area, EnCase
 - display of data decrypted from, 211
- Protected Storage System Provider area, decrypting, 236
 - with Cain, 237
- protocol analyzer, 147
- proxy servers, log from, 11
- psexec, 51
- PsFile utility, 137, 137
- PsList tool, 138, 138
- PsLoggedOn tool, 137, 138
- pulling the computer plug, 132
- pwdump2 tool, 82, 83–85
- pwdump3 tool, 83–85

Q

- Queensland Police Service, Forensic Computer Examination Unit, 211
- queries (SQL), 156
 - for account management events, 408–409
 - batch file to run, 321–323
 - broad, 396
 - for device drivers Event IDs, 420–421, 421
 - for Event ID 673 entries, 382
 - for Event ID 680 and 681 entries, 384
 - for Log Parser, 314–320
 - IN operator, 318
 - ORDER BY clause, 318
 - parts, 316
 - for stopped or started Security Center of Firewall, 419, 419
 - WHERE clauses, 318

questions
importance of, 7
for starting investigation, 4–5

R

rainbow table, 85
RainbowCrack, 82, 85
RAM. *See* memory
rcrack.exe, 85
Read Only attribute, 175
Read permission, for Everyone group, 42
reasonable doubt, 45
reconciling share and file permissions, 43–44
recovering event logs from free space, 446–451, 450
recovering files, after deleting, 171–172
Recycle Bin, for resolving SIDs to users, 233, 233
Red Cliff, 157
redirect operator (>), 145
regedit, 122, 195–200
Registry. *See also* HKEY_
basic concepts, 193–200
history, 195
bottom line, 212–213, 480–482
information in service, 121
“last known good configuration” for, 193
locations for starting code or program, 253–255
performing research, 201–202
Protected Storage System Provider area, 235

Restore point settings, 225–231
root-level keys, 196
user-level startup folder settings, 256
value data types, 200
viewing with forensic tools, 203–204
 AccessData’s Registry Viewer, 207–211, 208
 Encase, 204–207, 205
 Windows Firewall settings, 224
Registry Browser, 211
Registry editor, 195, 196
search feature, 200
Registry evidence
basics, 215–216
bottom line, 260–263, 482–485
IP addresses discovery, 246–249
LSA secrets, 245–246
restore point settings, 225–231
Security Center and Firewall settings, 220–224
security Identifiers (SIDs), 231–234
in software key, 216–220
 installed software, 216–218
 last logon, 218, 219
 logon banners, 219–220
startup locations for code, 253–258
time zone offsets, 251–253
user activity, 234–244
Registry Viewer (AccessData), 207–211, 208, 218
 Common Areas view, 209, 210
 demo mode limitations, 208
 for NTUSER.DAT file, 236
 Report function, 211
regmon.exe, 201, 274

- remote code execution, 46
 - remote connections, share permissions
 - for, 42
 - Remote Desktop, 388
 - Registry key value for, 212
 - Remote Desktop Protocol (RDP), 386, 388
 - port, 117
 - remote host (RHOST), 48
 - remote interactive logon, 46
 - remote resources, access to, 94
 - removable media, search warrant
 - for, 15
 - repairing corrupted event log
 - databases, **444–446**
 - \$REPARSE_POINT MFT attribute, 181
 - replay attack, 88
 - preventing, 386
 - reporting party, initial assessment of information from, 4
 - reports
 - creating narrative report with
 - hyperlinks, **455–460**
 - workflow tip, 462
 - electronic format for reports, **462–463**
 - importance of, 455
 - presenting, bottom line, 467–468, 498–500
 - timelines, **463–466**
 - resident data, 182
 - resources, controlling access to, 70
 - restore points, 226
 - creating for Windows XP, 194
 - disabling, 226
 - folders sorted by creation time
 - stamp attribute, 230
 - intruder’s tools in, 228
 - and MRUs, 239
 - names of, 226–227
 - retention period, default, for restore point, 225–226
 - rights, vs. policies or permissions, 38
 - rings, 70
 - rogue server, configuring for password cracking, 96
 - rogue wireless access points, 299
 - root user (Unix/Linux), 72
 - RootkitRevealer, 74
 - rootkits, 15, 17, **72–76**
 - embedding, 257
 - and live analysis results, 146
 - and port information, 112
 - Rootkits: Subverting the Windows Kernel* (Hoglund and Butler), 55
 - ROT-13 encoding, 241, 244
 - rotation of backups, and preserving evidence, 9
 - routers, connection logs from, 18
 - routing, for test network, 284
 - RPC Endpoint Mapper, port, 117
 - RPC over HTTP, port, 117
 - Run command, 142
- S**
- “sa” password (SQL), 265
 - SAFE (Secure Authentication for EnCase), 150
 - “salt,” adding to password, 81–82

- SAM database, 33
 - for SID-to-user resolution, 232
- samdump2, 103–105
- Sams Teach Yourself Networking in 24 Hours* (Habraken and Hayden), 108
- saving event logs, 339–340
- Scan Registry Enscript, 207, 207
- scanner, 17
- scanning
 - external ports, **284–285**
 - victim computers, **149**
- ScoopLM, 95
 - for cracking passwords, 98, 98–100, 99, 100
- screen display
 - photographing output, 143
 - sending to text file, 83
- search warrant, for digital evidence, 15, 16
- searching with Event Viewer, **347–351**
- SecEvent.evt file, database file
 - structure, 433–437, 435
- Secret Explorer, 236
- sectors, 165
- \$Secure file, 183
- Secure Global Catalog, port, 117
- Secure LDAP, port, 117
- Secure Shell, 110
- secure web traffic, Port 443 for, 320
- Security Account Manager (SAM), database, 33, 77
- security authority, 33
- Security Center, 220, 221
 - Alert Settings, 222, 222
 - setting changes by intruder, 221
- security, for Intranet web servers, 299
- security identifiers (SIDs), **231–234**
 - associating with volumes, in EnCase, 233
- SECURITY, \Policy\Secrets, 245
- security programs, and use with Kernel mode, 71
- Security Properties window, Filter tab, 348
- \$SECURITY_DESCRIPTOR MFT attribute, 180
- Security.evt log file, 327, 329
 - in Event Viewer, 335, 336, 337
- seizing suspect's computer, 15
- server, 22
- Server Message Block protocol, 42, 94–95, 97
- server operating system, versions, 24
- service accounts, 33, 400
- Service Control Manager, 118, 417–418
- Service Control Program, 118
- service ticket, 380–381
- ServiceDLL value, in Registry, 123, 124
- services
 - bottom line, 124–125, 475–477
 - in Kerberos vs. Microsoft term use, 375
 - one process for multiple, 121
 - vs. processes, 110
 - started in boot process, 224
 - in Windows, 110
- services text file, 114
- SGUIL, 148
- Shadow Drive, 273
- share permissions, 38, **42**
 - reconciling with file permissions, **42**

- shared code, libraries of, 56
- shell, 64
- shellcode, 64
- show exploits command (Metasploit), 47, 48
- show options command (Metasploit), 48, 50
- show payloads command (Metasploit), 48, 49
- shutdown
 - Event ID for, 319
 - graceful, vs. pulling cable, 132
- SID-to-user resolution, SAM database for, 232
- SIDs, Event Viewer interpretation of, 340–341, 341
- signature.gif file, 462
- Simple File Sharing, 39, 40
- Simple Mail Transfer Protocol (SMTP), port for, 108
- “single point of failure” vulnerability, of Registry, 193
- SMB over TCP, port, 116, 117
- Smith, Randy Franklin, 409
- SMTP (Simple Mail Transfer Protocol), port for, 108
- snapshot, of system by EnCase FIM, 153
- sniffer, 17, 46, 147
 - in Cain, 102
 - to capture authentication information, 95, 98–100
- Snort, 148
- social engineering, 16, 46
- source code, closed nature of, 18
- Source field, in event logs, 336
- source Internet Protocol (IP) address, 108
- source port, 108
- SPADA, 157
- speed in evidence analysis, need for, 14
- spoofed emails, with malicious software, 58
- SQL queries
 - for account management events, 408–409
 - batch file to run, 321–323
 - broad, 396
 - for device drivers Event IDs, 420–421, 421
 - for Event ID 673 entries, 382
 - for Event ID 680 and 681 entries, 384
 - for Log Parser, 314–320
 - IN operator, 318
 - ORDER BY clause, 318
 - parts, 316
 - for stopped or started Security Center of Firewall, 419, 419
 - WHERE clauses, 318
- SQL, running with administrator rights, 265
- SQL Server protocol, port, 117
- \$STANDARD_INFORMATION MFT attribute, 180, 181
 - file creation and, 184
- Start button
 - All Programs, Accessories
 - Communications, 388
 - System Tools, System Restore, 194, 226

- Control Panel
 - Administrative Tools, Internet Services Manager, 290
 - Network Connections, Local Area Connection, Internet Protocol (TCP/IP), 202
 - Security Center, 221
 - Windows Firewall, 222
 - MyComputer, Tools, Folder Options, 40
 - Start.exe file, 463
 - starting cluster, in FAT, 169, 169
 - startup locations for code, **253–258**
 - startups, autoruns to determine, 259–260, 260
 - static IP address, 248, 248
 - status byte, 170–171
 - storage, 56
 - streams.exe, 188
 - strings, tool analysis with, **268–270**
 - subroutines, 59
 - Success of action, logging, 331
 - Sun Tzu, 263
 - SuperScan, 149, 149
 - suspect computers, analyzing, **15–18**
 - svchost process, 121, 121
 - svchost.exe file, location for, 123
 - swap file, clear-text passwords in, 246
 - Sweep Case EnScript, 426
 - Sweep Enterprise EnScript, 153, 153
 - \$SYMBOLIC_LINK MFT attribute, 181
 - synchronizing database header and footer values, 445, 445
 - SysEvent.evt file, database file structure, 433–437, 435
 - Sysinternals
 - in FAT file, 167
 - Filemon tool, 133, 139, 141, 274, 277–278
 - psexec, 51
 - Regmon, 201, 274, 277–278
 - RootkitRevealer, 74
 - streams.exe, 188
 - strings program, 268–270, 269, 270
 - syskey, for decrypting SAM, 103–104
 - System attribute, 175
 - system events, logging events, 332
 - system files, displaying, 176
 - System Restore UI, types of restore points, 227
 - \System Volume Information folder, permissions for, 226
 - System.evt log file, 327, 329
 - in Event Viewer, 335, 335
 - examining events, **417–422**
 - File Extents view, 447
 - %SystemRoot%\ntds directory, 77
 - %SYSTEMROOT%\System32\config folder, 197
 - %SystemRoot% variable, 78
- T**
- target hash, 79
 - tasklist command, 118, 118
 - /SVC switch, 120, 120
 - for live analysis, 132
 - output from, 119
 - verbose output, 119, 120
 - Tasks folder, scheduled tasks in, 257
 - TCP (Transmission Control Protocol), 109

- tcpdump, 148
- technical matters, testifying about, **466–467**
- Technology Pathways
 - ProDiscover, 150
 - ZeroView, 140
- telephone, initiation of case by, 4
- Terminal Services, **387–392**
- test computers, for Windows live analysis CD, 133
- test environment
 - creating safe, 273–274
 - routing for, 284
- testifying
 - about technical matters, **466–467**
 - minimizing complexity for, 341
- text files, sending screen display to, 83
- Thernströmas, Pär, 312
- threads, 57, 58
- thumbs.db file, 164
- ticket-granting authority, 92
- Ticket Granting Ticket (TGT), 93
- Time applet, synchronizing, 447
- time period, for evidence search, 13
- time stamps, 129, 130
 - analysis, 75
 - decoding, 249
 - in Event Viewer, 336
 - for FAT, limitations, 174
 - for files, 173
 - for firewall settings, 224
 - in IIS logs, 291
 - for software, 218, 219
 - in Windows event logs, 337
- time zones, 207
 - compensating for offsets, **251–253**
 - in Event Viewer, 336
 - extracting from Registry, 206
 - offsets in event logs, 319
- timelines, in reports, 456, **463–466**
- TimeMap, 463, 464, 465
- timing of incident, 4
- Title III order, and monitoring system communications, 147
- tlist utility, 69
- Tools menu (Internet Explorer), Internet Options, Content, AutoComplete, 235
- tools of attacker, 263
 - monitoring network traffic from, **282–283, 283**
 - tools, in restore points, 228
- tools of intruder
 - action of, 266
 - analysis
 - basic steps, 276
 - bottom line, 286, 486–488
 - caution, 267
 - Dependency Walker, 263, **271–272**
 - monitoring code, **273–282**
 - monitoring network traffic from, **282–283, 283**
 - purpose of, **263–267**
 - with strings, **268–270**
 - external port scans, **284–285**
 - in restore points, 228
- topology of network, 6
- transflash cards, 16
- transitive trust relationships, example, 28–29

Transmission Control Protocol (TCP), 109
 ports, 117
.Trashes file, 164
Trojan program, 17
trust, in reported information, 8
trust relationship, 26
 example of, 28–29
.txt file extension, for saving event log, 340
Type field, in event logs, 335

U

UDP (User Datagram Protocol), 109
unallocated cluster, 167
“uninstall” key, for software, 217
United States Code, 18 USC 2703(f), 10
U.S. Department of Justice, Computer
 Crime and Intellectual Property
 Section, 147
universal groups, for domain
 controllers, 406
Universal Plug and Play protocol, port,
 117
Universal Time Coordinated (UTC),
 208, 251
\$UpCase file, 183
USA PATRIOT Act, 12, 147
USB drives, for live analysis, 143
use command (Metasploit), 48
User Assist area, 241, 242
User Datagram Protocol (UDP), 109
 ports, 116–117
User field, in event logs, 338, 349
User Mode, 70
username, for last logon, 218

users and groups
 account management logging,
 Windows 2000 vs. Windows
 Server 2003, 405
 assigning user to group, 34–35
 attacker creation of, 38
 deleting, 408
 disabled accounts, 33
 groups, 34–37
 investigating activity, 234–244
 types of accounts, 31–34
 users currently logged on, 137, 138
UTC (Universal Time Coordinated),
 208, 251

V

values in Registry, 195
variables, 57
vendors, patches from, 45
vetting, initial, 3–5
victim computers
 avoiding tool use on, 132, 144
 evidence from, 215
 for intruder toolbox, 264
 watching to catch intruder, 266
 logs from, 12
 minimizing impact of live analysis
 on, 142
 monitoring communication with,
 146–148, 147
 running rogue servers on, 111
 scanning, 149
victim organization
 meeting with, 5–10
 theory of crime, 7

- virtual machine
 - cloning, 280–281
 - for testing, 273
- virtual network computing (VNC)
 - server, 68
- Virtual PC, 134, 273
- virus protection
 - disabling, 224
 - and malware tool, 277
 - and tool analysis, 267
- VMWare, 103, 134, 273
 - EnCase to examine virtual machine image file, 280
 - snapshot of baseline testing environment, 276
- VNC (virtual network computing)
 - server, 68
 - Application log login information for, 422
- \$Volume file, 183
- \$VOLUME_INFORMATION MFT attribute, 181
- \$VOLUME_NAME MFT attribute, 181
- volumes, associating security ID with, in EnCase, 233
- \$VOLUME_VERSION attribute, 180
- Voom Technologies, 273
- vulnerability, exploiting, 46

W

- W3C Extended Log File Format
 - fields for IIS logs, 293–294
 - for Firewall log file, 320
 - for FTP log, 302
 - sc-status field, error codes, 294–296

- W3C Extended Log File Format setting, for IIS log, 291–298
- web pages, to cause authentication attempt, 97
- web resources
 - on current rootkit projects, 73
 - on network monitoring, 148
- web server, 110
 - intranet, security for, 299
- well-known ports, 108, 109, 110, 116
- Wetstone Technologies, LiveWire Investigator, 150
- WHERE clauses, in Log Parser query, 318
- Whoami tool, 136, 136
- Wilson, Craig, 249
- win32_bind payload, 49
- Windows
 - authentication mechanisms, 87–93
 - AutoStart method, 255
 - Encrypting File System (EFS), 102–103
 - recovering files encrypted with, 102–103
 - graphical user interface (GUI), 55
 - live-analysis CDs, 131–145
 - burning, 136
 - creating for Windows XP, 134–136
 - dynamic-link libraries (DLLs), 133
 - preparing tool copies, 135
 - selecting tools for, 133–138
 - using, 142–145
 - verifying, 139–140
 - logging decentralization, 360

- metadata files from, 164
- password storage in, 77–78
- services, 117–124
- versions, 161, 162
 - and log analysis, 395
 - numbers, 22
- Windows 2000
 - domain controller in, 24
 - event log analysis, 361–386
 - comparing logon and account logon events, 361–364
 - examining events, 364–366
 - vs. Windows XP logging, 386–392
- Windows 2000 Server, 22
 - Metasploit to break into, 47
- Windows accounts, disabling vs. deleting, 359
- Windows authentication, sniffing and cracking exchanges, 94–95
- Windows domains, 23–29
 - interconnecting domains, 25–27
- Windows Event Log Parser, Setup tab, 427
- Windows event logs, 327–334. *See also* Microsoft Log Parser
 - auditing settings, 329–334
 - bottom line, 453, 492–493, 496–498
 - database record fields - raw, 441–442
 - EnCase to examine, 425–433, 426
 - field names, 443
 - filtering, 347–349
 - finding and recovering from free space, 446–451, 450
 - folder for, 197
 - internals, 433–444
 - open and not synchronized, 440
 - opening, 342, 342–343, 343
 - parsing fragments with EnCase, 452, 452
 - record, 441
 - repairing corrupted databases, 444–446
 - reports of analysis, 346
 - starting and stopping of service, 421
 - time stamps in, 337
- Windows Firewall, 220
 - accessing, 222
 - Event log record showing stopped, 418, 418
 - General Tab options, 223
 - list of globally open ports, 225
 - logs, 310–312
 - query of, 320
 - remnants in slack space, 434
 - Registry settings, 224
- Windows Initialize Case EnScript, 206
 - for determining which software is installed, 218
- Windows NT
 - domain controller in, 24
 - Event IDs for logons, 354
 - NTFS (New Technology Filesystem), 177–186
 - Rescue floppy disks, 77
- Windows NT Advanced Server, 22
- Windows NT logon events, 353–361
- Windows Registry. *See* Registry
- Windows Server 2003, 22
 - account logon and logon events, 393–395

- cracking passwords, on domain controller, 83–87
 - principles for analyzing, 396
 - viewing event logs on Windows XP, 342
 - Windows Vista, viii
 - Windows XP
 - creating restore point in, 194
 - default directory structure for, 163, 165
 - Service Pack 2, 220
 - Terminal Services in, 388
 - viewing Windows Server 2003 logs on, 342
 - vs. Windows 2000 logging, 386–392
 - Windows XP Professional, installing IIS on, 290
 - WinHex, 165
 - report, 165
 - winpcap.dll, 268
 - wireless access, by former employee, 298–299
 - wireless routers, DHCP logs from, 309
 - Wireless Zero Configuration Service (WZCSVC), 250
 - Wireshark, 17, 148, 274
 - Word (Microsoft), 457
 - workgroups, 23
 - workstation computers, 22
 - Workstation Name entry, in Event Properties description, 355
 - wsock32.dll, 268
 - WZCSVC (Wireless Zero Configuration Service), 250
- Y**
- Yahoo toolbar, searches stored in Registry for, 240, 241
- Z**
- ZeroView, 140
 - Zulu Time, 208